Remarks

This communication is responsive to the Non-Final Office Action of **February 19, 2009**. Reexamination and reconsideration of the remaining claims is respectfully requested.

Status of Claims

Claims 1, 6-20, 41, and 46-60 are pending for examination.

Claims 1, 6-20, 41, and 46-60 are amended herein.

Claims 1 and 41 are in independent form.

Summary of The Office Action

Claims 1, 6-20, 41, and 46-60 were rejected under 35 USC §103(a) as purportedly being anticipated by Carter et al. (US 2003/0051026)(Carter) in view of Rokosz (US 7092866)(Rokosz).

Response

The Claims Patentably Distinguish Over the References of Record

35 U.S.C. §103

Claims 1, 6-20, 41, and 46-60 were rejected under 35 USC 103(a) as purportedly being anticipated by Carter in view of Rokosz. To establish a prima facie case of 35 U.S.C. §103 obviousness, basic criteria must be met. The prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP 2143.(A) Section 2131 of the MPEP recites how "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). This same standard applies to 103 rejections as evidenced by Section 2143(A) of the MPEP, which reads: "The rationale to support a conclusion that the claim would have been obvious is that **all the claimed elements** were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions".

When establishing a prima facie case of obviousness the Office must clearly articulate the reason(s) the claimed invention would have been obvious. MPEP 2142 recites that:

> The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___, 82 USPQ2d 1385, 1396 (2007) noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal

> conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). See also *KSR,* 550 U.S. at ___ , 82 USPQ2d at 1396 (quoting Federal Circuit statement with approval).

Additionally, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). This requirement is intended to prevent unacceptable "hindsight reconstruction" where Applicant's invention is recreated from references using the Application as a blueprint.

Here, the criteria for establishing a prima facie case of obviousness are not satisfied since the combination of references does not teach or suggest all the claim limitations. None of the references, alone and/or in combination, teach an event-driven reference monitor **simulator** that operates at least partially at the **kernel level** and that can operate faster than an actual reference monitor. The combination of references describes a network surveillance and security system (Carter) that interacts with a method for time compression during software testing (Rokosz). It is unclear what, if anything, would be created by combining the references. Carter is at least concerned with computer security, but it is not a simulator, it cannot be made to run faster than real time, does not run any portion in the kernel, and is not event driven. Rokosz describes how to detach an application from a system clock by using a fake clock to facilitate doing months worth of software testing in a few days. Rokosz is not associated with computer security, is not event driven, and does not run any portion in the kernel. Thus, none of the claims are obvious for at least this reason.

Claims 1 and 46

Carter describes a system that monitors and protects the security of computer networks using artificial intelligence, including learning algorithms, neural networks, and genetic programming. The Office Action admits that "Carter does not explicitly disclose controlling the reference monitor simulator to operate at an accelerated rate." Page 4. In addition to not disclosing a reference monitor simulator operating at an accelerated rate, Carter does not appear to teach a reference monitor simulator at all. Carter appears to teach a real-time network security system, but no reference monitor **simulator**. Rokosz clearly does not teach a reference monitor simulator. Thus, for at least this reason the independent claims are not obvious over the combination of references.

The Office Action asserts that Rokosz teaches controlling the reference monitor simulator to operate at an accelerated rate. This is incorrect when viewed in context of the claim, especially the amended claim. The claim recites "controlling the reference monitor simulator to operate at an accelerated rate ... by providing at least one parameter ... [that] controls one or more of, eliminating a time gap between trace requests, indicating that a time period between portions of a trace request has elapsed, and running a system clock faster than real-time". None of these elements are found in either Carter or Rokosz.

The amended claim recites how the method operates at least partially in the **kernel** and is **event-driven**. Support for these amendments appears on at least page 6, lines 15-19 and page 7, lines 16-31. Both Rokosz and Carter appear to operate only at the application level, not dipping down into the kernel level. Furthermore, neither Rokosz nor Carter appear to be event driven.

Concerning the independent claims before amendment, the Office Action asserts that Rokosz column 11, lines 44-61 teaches all the elements. This is

incorrect. This passage teaches how modules to support time compression testing can be built into an application under test. The application has nothing to do with trace requests. The application is not a reference monitor simulator. Once the modules are built into the software application under test, then time compression testing can occur. While time compression is possible, it does not teach the claimed method of providing a parameter that controls eliminating a time gap between trace request, indicating that a time period between portions of a trace request has elapsed, or running a system clock faster than normal. Neither reference provides the claimed parameter.

The time compression in Rokosz involves producing a "fast time mode that is **detached** from the system clock." A clock modification module is placed into an abstraction layer to hide calls to time functions in the operating system. Rokosz specifically requires that the system clock of the operating system not be updated. However, the claim includes "running a system clock faster than real-time." A reference whose time compression explicitly disclaims updating the system clock and that explicitly detaches fast time from the system clock cannot possibly teach "running a system clock faster than real time." So, neither reference teaches anything to do with trace requests. Additionally, neither reference teaches providing the time parameter. Therefore it follows that neither reference teaches operating at an accelerated rate by using the missing time parameter to manipulate gaps and time periods associated with the missing trace requests. Thus the independent claims are not obvious over the combination of references even before the amendments.

The amendments recite event-driven operation occurring at least partially in the kernel. Rokosz teaches building things into a software application. Things in a software application do not operate at the kernel level as now claimed. Thus, for at

least this additional reason the independent claims are not obvious and are in condition for allowance.

Accordingly, none of the dependant claims are obvious for at least the same reasons and are, therefore, in condition for allowance.

Claims (6,46), (7,47), (8,48)

These claims depend from allowable claims and are therefore allowable for at least the same reasons. However, these claims recite additional elements and limitations that are not taught by the references. These claims concern assessing the effectiveness of security rules. Rokosz is silent concerning security rules and thus only Carter is used to purportedly teach assessing the effectiveness of security rules. However, Carter is completely silent about assessing the effectiveness of security rules.

The Office Action asserts that Carter [0222] and [0260] teaches assessing the effectiveness of security rules. This is incorrect. Paragraph [0222] merely describes how the system tries to block access. There is no assessment of the effectiveness of the rule. Paragraph [0260] merely describes how the system uses neural networks to learn new rules without saying anything about assessment of current rules. Simply describing that the system may block access or may use neural networks to learn new rules falls well short of making a prima facie case for obviousness of a claim that includes assessing the effectiveness of a security rule. For this additional reason claims 6 and 46 are not obvious and are in condition for allowance.

The Office Action asserts that Carter [0260], [0606-611], and [0802] teach assessing the effectiveness of security rules by determining the number of improper requests presented and the number of proper requests allowed. This is also incorrect. [0260] only teaches that the system uses neural networks. It is completely silent about determining the number of improper requests. [0606-0611] only teaches how policies can be expanded or revised, but says nothing about assessing rules. Similarly, [0802] merely describes a watchdog process. The paragraph is silent concerning assessing rules. Applicant respectfully requests a quotation from the reference that even mentions the words "effectiveness of security

rule". No such quotation can be found. For this additional reason claims 7 and 47 are not obvious and are in condition for allowance.

The Office Action asserts that Carter [0403] and [0411-413] teach assessing the effectiveness of a security rule by determining a rate of improper requests received. This is incorrect. These paragraphs describe observing a system and describe how many neurons are used in the observing. These paragraphs also describe comparing the probability of detection to the probability of a false alarm. There is absolutely nothing about rates. Indeed, the word "rate" does not appear in any of the paragraphs as detailed below. Applicant respectfully requests a citation to the portion of the reference that describes the claimed rates. Sentence by sentence analysis of the cited portions of the reference yield absolutely nothing to do with any rate, let alone assessing effectiveness by determining a rate of improper requests received.

Sentence in [0403]	Rate?
Measurements of the system,	No
obtained by monitoring output from UNIX process	No
designed to observe the protected environment.	No
This form of knowledge is referred to as observations.	No
The term observables refers to points of observation.	No
Ordinarily, these observations are inherently prone to errors in observables,	No
being subject to monitoring errors and estimation imperfections.	No
The observations provide the information for the examples used to train the learning by the Neural	No

Network.	
Sentence in 0411	Rate?
The number of neurons involved in the representation of a quality corresponds to the importance of that quality to the learning goals.	No
Correlating the number of neurons involved in a representation with the importance of the item being represented is well known in the art.	No
Detecting an attack in the midst of other system activities is an important goal of the neural network.	No
The caliber of performance of attack detection is measured in terms of two probabilities:	No
Sentence in 412	Rate?
Probability of detection,	No
defined as the probability that the system correctly determines an attack is imminent or occurring	No
Sentence in 413	Rate?
Probability of a false alarm,	No
defined as the probability that the system incorrectly determines an attack is imminent or occurring.	No

Thus, claims 8 and 48 are not obvious for at least this additional reason.

Conclusion

For the reasons set forth above, the remaining claims are now in condition for allowance. An early allowance of the claims is earnestly solicited.

Respectfully submitted,

Date: April 28, 2009

John T. Kalnay (Reg. No. 46,816)
(216) 308-3245
(216) 503-5401 (fax)
Kraguljac & Kalnay, LLC
Summit One, Suite 510
4700 Rockside Road.
Independence, OH 44131